An Ethics Whirlwind: A Perspective of the Digital Lifestyle of Digital Natives and Initial Thoughts on Ethics Education in Technology

Brian R. Hall
hall@champlain.edu
Division of Information Technology & Sciences,
Champlain College
Burlington, VT 05402, USA

Abstract

As digital natives continue rolling onto college campuses around the country, the questions surrounding digital ethics grow. Students do not know life without modern technology, computers, mobile devices, the Internet and their lifestyle has developed around this mass. Unlike their predecessors, they do not recognize a difference between the digital space and the real world. They are one-in-the-same. Yet, the connection between digital actions and real-life consequences is often unrecognized. This is mainly due to the fundamental lack of proper moral code education and application. This paper is a presentation of data collected on students' digital behavior and initial thoughts on the issues surrounding digital ethics education.

Keywords: ethics, digital lifestyle, technology education, behavior, moral framework

1. INTRODUCTION

To lay the foundation for further study on digital ethics education an initial questionnaire was developed and distributed to three same-semester sections of an introductory web class at a teaching college in New England. The rationale behind the class selection was threefold: introductory web classes have a good mix of technology majors, the majority of students would be first-year and such a web class incorporates a large mix of technological issues – networks, the Internet, social networking, security, publication, privacy, programming, media and so on. For a sample non-technologist comparison the questionnaire was also given to a section of criminal justice majors.

There are several goals for the multi-part study. This first component, and paper, provides data on some digital behaviors and ethical viewpoints of students. The derived information will assist in developing a deeper examination and determination as to what incoming students view as ethical digital behavior. Also, it must be determined to what extent behavioral differences exist between the digital space and non-digital aspects of life and decision-making. Another part of future study will be assessing the state of ethics education in technology programs around the country and its emphasis in model curricula.

Eventually, the empirical evidence will be used to help establish a model for properly educating technology students, and retraining them if necessary, on the topic of an ethical digital lifestyle. This should also result in the application of ethical and moral principles to objectives of technologists. The primary challenge with this type of research is keeping pace with the technology (Peslak, 2007, p. 1).

2. LITERATURE AND QUESTIONS

There have been many studies and thoughts presented in the past on students' software piracy and morals (Kini, Rominger & Vijayaraman, 2000; Ramakrishna, Kini & Vijayaraman, 2001), computer security practices (Teer, S. Kruck & G. Kruck, 2007), attitudes toward computers and software (Anderson & Schwager, 2002), risky computing practices (Aytes & Connolly, 2004), careless views on privacy (Hinde, 2003), how to improve user behavior (Lu & Lin, 1998/1999; Collins, Rawlinson, Manwani & Allen, 2005; Leach, 2003), and even ethical views of students vs. professionals in information systems scenarios (Cappel & Windsor, 1998). There are entire journals in the information and technology field devoted to ethical topics (e.g. *Ethics and Information Technology*).

The common academic approach has been to separate these technology topics and research specific reasons for a specific behavior, and to suggest methods for improving specific outcomes. For example, one can easily find articles on ethics of computer and information security, but few on student behavior and perceptions surrounding a digital *lifestyle*. Though the scientific and philosophical methodology of breaking things into their smallest components may be useful to a certain extent, it may not be the best approach to the subject of digital behavior and ethics.

An alternative approach in the professional world has been to push the "code of ethics" doctrine (ACM, IEEE, AITP, etc.). Unfortunately this strategy has not been extremely influential in education, and is conflicted and volatile (Peslak, 2007). So, even *if* organizations adopt some sort of umbrella ethical code about information and technology, it does little for purposeful education or altering the digital decision-making of those raised with modern technology. Does the world expect students, future technology professionals, to instantly apply a code of ethics that differs from their established beliefs and behaviors?

A current observation is that one way ethics is detached from the classroom is its virtual non-existence in the IS model curriculum (Topi et al., 2009). It is slightly more emphasized in the IT and CS curriculum models, but still lacks a cohesive, unambiguous and fundamental tone (Lunt et al., 2008; Cassel et al., 2008). As already alluded to, a curriculum analysis will be conducted in a future phase of this research. Still, the ongoing challenge is to find the best approach to educating students on this topic.

The main research questions to be approached throughout the study are as follows:

RQ1: What are the digital behaviors and ethical views of students entering college?

RQ2: What do students perceive as acceptable or troublesome digital behavior?

RQ3: What are the implications of these behaviors and perceptions?

RQ4: What is the current state of ethics in the classroom?

RQ5: How should technology educators educate or retrain students about digital ethics?

This paper primarily addresses RQ1, and partially confronts RQ2 and RQ3.

3. METHODOLOGY

Abstraction is extremely important in many areas of computer science, particularly in algorithm design, computer organization/architecture, and complex systems (e.g. biological, neural networks, robotics). Taking an elevated view can be very beneficial when studying highly complex systems and in understanding how something works and why (Schneider, Gersting & Miller, 2009). For example, discussing how computers work in terms of electronic gates does little to educate many, if not most students. Alternatively, it is much more engaging to discuss how a CPU communicates with memory or how multiple information systems work together architecturally.

The fact that current and future students have not been raised alongside computing technology, but every aspect of their life has been intertwined with it makes the issue quite complex. Possibly more complex than it is with digital immigrants, those who were introduced to such things later in life. Therefore, viewing digital behavior at a higher level, as a lifestyle, can be an advantageous approach.

With this high-level abstraction (HLA) methodology in mind, the first-phase questionnaire was developed with the understanding that the natural tendency of digital natives, those raised surrounded by tools of the digital age, is to view technology in terms of *use* rather than what is happening

technologically (Prensky, 2001). This had an impact on the questions chosen and their wording. The survey provided the quantitative data discussed in this paper.

The questionnaire was a set of 20 questions to which the students could respond *Yes, No,* and if applicable *Some*. Their year status was also obtained. In total the questionnaire was given to 69 students. The primary group totaled 59 students composed of 45 freshmen, 2 sophomores, 4 juniors and 8 seniors/continuing studies. The smaller comparison group of 10 criminal justice majors was only meant to be a sample (not of high statistical significance) that might give non-technical yet related insight into the topic.

4. RESULTS

Aside from the following discussion, the full survey (Table 1) and results (Table 2) are included in the Appendix. An admonition to readers of this paper is to be mindful that this is one instance of student perspective. It is very possible that results would vary based on location, variations in student year-status and nationality, and the distribution numbers and date.

The results were a mixture of expected, unexpected and telling. When broken out, the questions fall into different categories (Table 3) that may be considered aspects of the digital lifestyle: attention, recipient, actions/behavior, privacy, and belief. Some questions may contribute to more than one category; not all combinations have been declared. There are many other questions that could have been part of this initial questionnaire, but again the goal was to get an overall sense of the digital lifestyle, not to dissect individual categories or questions.

Attention

The goal of the *Attention* category was to get a feel for the level of attention paid to digital detail. Sometimes detail in the digital space can be technological in nature such as a warning prompting the installation of a file. Sometimes it can be legal detail such as in the case of End User License Agreements (EULAs). And sometimes it can be noticing when someone is being emotionally or verbally attacked via a technological medium, which crosses into some of the other categories.

The questions posed in this category netted expected yet somewhat conflicting ideas. Nearly 40% do not give attention to security certificates and likewise nearly 50% to Terms of Service (TOS). As expected EULAs get the least amount of attention with 78% not reading applicable agreements. Yet, 83% do read prompts and warnings before clicking. The only major difference with the sample non-technologist group was they were even less likely to read the warnings and TOS agreements.

Naturally, this progression of likelihood of attention to detail is linked to the length and complexity of the information. As with most people, information is expected in a distilled and quickly digestible format. This is something that composers of the information and its presentation must incessantly remember. However, regardless of length or complexity, educators should dedicate more resources to the importance of attention to detail in the digital space. The belief that technology and systems make our lives easier should not equate to indifference. An EULA may not be a space heater, but reading the warning label may prevent “burning the house to the ground”.

Recipient

One of the questions that might apply to both the *Attention* and *Recipient* categories was if the student had witnessed the attempted reputation damage of another person via some form of technology. This would include things such as status updates on social networking sites, email, web postings, digital photos, and is inclusive of the larger topic of cyber-bullying. In the primary group 65% of students claimed to have seen this behavior and 70% in the secondary group.

There were two other questions posed in which the student was a direct recipient. The results of these questions also give cause for concern. First, 30% reported being on the receiving end of what they considered harassing messages through social networking sites. In the comparison group it was 50%. Second, in both groups 60% of students indicated that they had not been exposed to discussions of ethical digital behavior in high school. This may be changing in many places, but obviously it is still an area that needs more attention.

One of the responsibilities of collegiate educators, even in technical fields, is to create well-rounded global citizens. If students are not receiving proper ethics instruction prior to college, when most behaviors are established, then it is critical the subject is delivered with

directed intensity. It must be repeatedly expressed that digital behavior is not abstract and it is not virtual. It is real and therefore has real consequences. Technology and systems are catalysts for many things, but the sense of a virtual or digital existence is giving rise to an unwarranted sense of behavioral entitlement that does not expect actual consequences.

Actions

A large portion of the questionnaire was designed to ascertain the *Actions* of incoming students in the digital space. These eight questions varied greatly in focus, again to gain an overall sense of usage of technology and systems. The results of the criminal justice group were similar to the technologist group aside from them being slightly less likely to illegally download media or install pirated software.

In sum: 92% had downloaded pirated media, 66% had taken content from the web and used it without citing credit, 85% had used an Internet connection they were unauthorized to use, 85% had installed pirated software on their computers, and 63% had seen someone doing something they considered "wrong" on a computer and took no action against it. One of the redeeming statistics was that 95% claimed they had not attempted to damage another person's reputation using forms of technology. A couple of the questions that blend into the next category of *Privacy* were that 34% had looked through someone else's computer, files or email, and 70% had tried to find information about someone for personal reasons using technological means.

This group of questions was also one of the drivers for the selection of first-year criminal justice majors as the secondary sample group. Most of these actions could result in legal action, some civil and some criminal, so getting their case was useful. There is definitely a lack of awareness, a feeling of indifference, or a logical detachment between digital actions and tangible outcomes. Digital natives, students and many other people in general do not know of, consider, or in some cases care about the existing laws governing digital behavior.

Take the cases of 85% using an unauthorized network connection and 34% looking through someone else's computer and apply it to the following Vermont Statute (13 VSA, 2011).

> "Title 13: Crimes and Criminal Procedure, Chapter 87: Computer Crimes
>
> § 4102. Unauthorized access
>
> A person who knowingly and intentionally and without lawful authority, accesses any computer, computer system, computer network, computer software, computer program, or data contained in such computer, computer system, computer program, or computer network shall be imprisoned not more than six months or fined not more than $500.00, or both. (Added 1999, No. 35, § 1.)"

Simply put, the education of digital ethics and consequences is not pervasive.

Privacy

Several of the questions were focused on *Privacy* concerns. Like most topics ethics is wrapped in the web of perception, so to help this study it is necessary to determine what the perception is of personal information and its digital availability. 57% of students either had no or only some concern about personal information available via the Internet. 50% are willing to leave computers "logged in" for extended periods of time. However, 90% use some form of privacy granulation and 56% do not use public computers for personal reasons. The non-technical group was even less concerned about information availability, but was more guarded about leaving account sessions active.

These results show another conflict. Though students are mostly unconcerned with their personal information being digitally available, they do care about being able to control it in some way. This suggests they are mildly aware that there is potential danger in the misuse of or unethical actions based on their digital information. On an anecdotal level it could be stated that these numbers would be very different if more of them had been personally or professionally burnt by the misuse of their digital information or if they knew exactly what information *is* available. Particularly with about 50% leaving accounts active or using public computers for personal reasons.

As educators one concern should be raising awareness of ethics and information privacy of a digitized life. For example, if students discussed the availability of their legal records on their respective county clerk web sites, they

would begin to consider not only its unrestricted availability, but also their actions leading to its digital existence and the morality of its usage by potential employers when making hiring decisions. The problem is that many are not even aware this does exist. Even more important, such topics should be discussed to inform the moral compasses of the students who will be responsible for building and maintaining such systems.

Belief

The last category, *Belief*, had one main question though some of the previously discussed questions percolate into this area. One example was the question in the *Actions* section that asked if the student had seen someone doing something "wrong" and did not take action against the behavior. Such a question is based on what the student believes to be wrong. Be that as it may, the pivotal question was direct and asked if the student applied the same moral, ethical and legal beliefs digitally that they believe in otherwise. The telling response was that nearly 50% either do not or only partially.

This data highlights the failure or complete lack of digital ethics education for students throughout the evolution of digital technology, the Internet and its applications. Furthermore, what was and is an oversight in education has fostered unethical social norms that incoming students have adopted. An ethical and moral framework was never a *principal* concern and it is still an afterthought in most technology programs.

In most cases there may be one ethics course in a program, sometimes technology ethics, often only included to meet accreditation requirements. At that point hands are wiped clean and it is claimed that moral responsibility has been met. This method is dangerous and only reinforces the mentality that ethics is 'easy' and not fundamental in the digital age (Cassel et al., 2008, p. 92).

At the 2011 TEDx Silicon Valley event, Damon Horowitz stated that technology makers should be considering their "moral operating system" just as much as their mobile operating system and that "we have stronger opinions about our handheld devices than the moral framework we should use to guide our decisions" (Horowitz, 2011). Technology educators must be more proactive in confronting this issue and the earlier the education the better.

5. CONCLUSIONS AND FUTURE RESEARCH

This first step of gaining an understanding of the current state of students entering higher education, particularly in the technology field, was important for the final goal of the multi-part study. That goal is to develop a better method of educating technology students on the subject of digital ethics. Though this is important for all students, it is even more important for those responsible for designing and building the systems and solutions to meet the needs of the digital era.

It must be understood that this will not be an attempt to "tack on" the mere idea of good-faith adherence to a code of ethics or to suggest a "quick fix" course. This developing method will strive to supplement the entire educational experience and fundamentally change how students digitally live. The next phases of behavior examination and exploration of ethics content in IS/IT/CS programs should give a better view of the moral mindset of students and their ethics exposure. This ongoing research will also provide content for ethics extensions to ACM and AIS model curricula and associated wikis.

Technology educators have a heightened responsibility as a result of technology evolution. Technology educators should intently be focusing on developing an appropriate and modern method for building and reinforcing a moral framework for this new type of student, the digital space and the information age.

6. REFERENCES

13 Vt. Stat. Ann. ch.87 § 4102 (2011). LexisNexis.

Anderson, J., & Schwager, P. (2002). Security in the Information Systems Curriculum: Identification & Status of Relevant Issues. *The Journal of Computer Information Systems*. 42(3), 16-24.

Aytes, K., & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing*. 16(3), 22-40.

Cappel, J., & Windsor, J. (1998). A Comparative Investigation of Ethical Decision Making: Information Systems Professionals versus Students. *The DATA BASE for Advances in Information Systems*. 29(2), 20-34.

Cassel, L., Clements, A., Davies, G., Guzdial, M., McCauley, R., McGettrick, A., Sloan, B., Snyder, L., Tymann, P., Weide, B. (2008). Computer Science Curriculum 2008: An Interim Revision of CS 2001. ACM & IEEE.

Collins, B., Rawlinson, R., Manwani, S., & Allen, K. (2005). How Can We Spread The Security Message?. *Computer Weekly*. 32.

Duffy, T., & Walstrom, K. (2003). Changes In Student Computer Technology Attitudes Over Time. *The Journal of Computer Information Systems*. 43(3), 27-33.

Hinde, S. (2003). Careless About Privacy. *Computers & Security*. 22(4), 284-288.

Horowitz, D. (2011, May 14). Responsibility With Data. *Tedx Silicon Valley: Living by Numbers*. Retrieved from: Live Webcast http://www.tedxsv.org/?page_id=98 and Blog http://www.tedxsv.org/?p=1135 and Third-Party http://venturebeat.com/2011/05/14/damon-horowitz-moral-operating-system/

Kini, R., Rominger, A., & Vijayaraman, B. (2000). An Empirical Study of Software Piracy and Moral Intensity Among University Students. *The Journal of Computer Information Systems*. 40(3), 62-72.

Leach, J. (2003). Improving User Security Behavior. *Computers & Security*. 22(8), 685-692.

Lu, Hsi-Peng & Lin, Jien-Liang (Winter 1998/1999). Effects of Learning and Living on IS Ethics Education. *The Journal of Computer Information Systems*. 39(2), 96-100.

Lunt, B., Ekstrom, J., Gorka, S., Hislop, G., Kamali, R., Lawson, E., LeBlanc, R., Miller, J., Reichgelt, H. (2008). Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. ACM & IEEE.

Peslak, A. (2007). A Review of the Impact of ACM Code of Conduct on Information Technology Moral Judgment and Intent. *The Journal of Computer Information Systems*. 47(3), 1-10.

Prensky, M. (2001). Digital Natives, Digital Immigrants. *On The Horizon*. 9(5). MCB University Press.

Ramakrishna, H., Kini, R., & Vijayaraman, B. (2001). Shaping of Moral Intensity Regarding Software Piracy in University Students: Immediate Community Effects. *The Journal of Computer Information Systems*. 41(4), 47-51.

Schneider, G., Gersting, J., & Miller, K. (2010). *Invitation to Computer Science, 5th ed*. Boston, MA: Course Technology, Cengage Learning.

Teer, F., Kruck, S., & Kruck, G. (2007). Empirical Study of Students' Computer Security Practices/Perceptions. *The Journal of Computer Information Systems*. 47(3), 105-110.

Topi, H., Valacich, J., Wright, R., Kaiser, K., Nunamaker, Jr. J., Sipior, J., & Vreede, G. (2009). IS 2010 Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. ACM & AIS.

Appendix

Table 1: Survey

Question	Yes	No	Some
Do you pay attention to security certificates?			
Do you use privacy granulation or attempt to control who can see particular information about you on the Internet? (eg. friend lists in Facebook)			
Do you read EULAs (End User License Agreements, when Installing software)?			
Have you ever received a harassing message through a social networking site?			n/a
Do you read warnings, prompts, before clicking Yes/No?			
Have you ever downloaded music/movies/media without paying for it?			n/a
Have you used text/code/images from the internet without citing credit?			n/a
Have you attempted to find information on an individual for personal reasons?			n/a
Have you used someone else's unsecured wireless connection?			n/a
Have you looked through someone else's email/account/files/computer?			n/a
Are you concerned about the amount of information about you available on the Internet?			
Have you ever installed software you didn't purchase (excluding Freeware, Open Source, etc)?			n/a
Have you ever tried to damage someone's reputation using some form of technology (status updates, web page, mass email, posting pictures)?			n/a
Have you ever seen the above done to someone, but weren't involved?			n/a
Do you read the Terms of Service when you sign-up online for a service (like google sites, web hosting, email account, online banking)?			
Do you apply the same moral, ethical, and legal beliefs digitally that you believe in otherwise?			
Did any teachers in high school discuss questions like those addressed in this survey?			n/a
Have you ever seen someone else doing something "wrong" on a computer and said nothing to them or a teacher/supervisor/manager?			n/a
Do you use public computers for personal reasons?			
Do you set your email or other accounts to stay "signed in" for extended periods of time?			

Circle your year in College: Freshman Sophomore Junior Senior Grad/CP

Table 2: Results

	Primary Group (n=59)				Secondary Group (non-technologist, n=10)		
Question	Yes %	No %	Some %		Yes %	No %	Some %
Do you pay attention to security certificates?	15.25%	37.29%	47.46%		30%	50%	20%
Do you use privacy granulation or attempt to control who can see particular information about you on the Internet? (e.g. friend lists in Facebook)	81.36%	10.17%	8.47%		80%	0%	20%
Do you read EULAs (End User License Agreements) when installing software?	3.39%	77.79%	18.64%		0%	80%	20%
Have you ever received a harassing message through a social networking site?	30.51%	69.48%	n/a		50%	50%	n/a
Do you read warnings, prompts, before clicking Yes/No?	83.05%	6.78%	10.17%		50%	10%	40%
Have you ever downloaded music/movies/media without paying for it?	91.53%	8.47%	n/a		80%	20%	n/a
Have you used text/code/images from the Internet without citing credit?	66.10%	33.90%	n/a		70%	30%	n/a
Have you attempted to find information on an individual for personal reasons, using the Internet?	69.49%	30.51%	n/a		70%	30%	n/a
Have you used someone else's unsecured wireless connection?	84.75%	15.25%	n/a		70%	30%	n/a
Have you looked through someone else's email/account/files/computer?	33.90%	66.10%	n/a		40%	60%	n/a
Are you concerned about the amount of information about you available on the Internet?	42.37%	45.76%	11.86%		10%	60%	30%
Have you ever installed software you didn't purchase (excluding Freeware, Open Source, etc.)?	84.75%	15.25%	n/a		50%	50%	n/a
Have you ever tried to damage someone's reputation using some form of technology (status updates, web page, mass email, posting pictures)?	5.08%	94.92%	n/a		10%	90%	n/a
Have you ever seen the above done to someone, but weren't involved?	64.41%	35.59%	n/a		70%	30%	n/a
Do you read the Terms of Service when you sign up online for a service (like Google Sites, web hosting, email account, online banking)?	18.64%	47.46%	33.90%		0%	70%	30%
Do you apply the same moral, ethical and legal beliefs digitally that you believe in otherwise?	52.54%	27.12%	20.34%		60%	20%	20%
Did any teachers in high school discuss questions like those addressed in this survey?	40.68%	59.32%	n/a		40%	60%	n/a
Have you ever seen someone else doing something "wrong" on a computer and said nothing to them or a teacher/supervisor/manager?	62.71%	37.29%	n/a		50%	50%	n/a
Do you use public computers for personal reasons?	33.90%	55.93%	10.17%		40%	60%	0%
Do you set your email or other accounts to stay "signed in" for extended periods of time?	42.37%	50.85%	6.78%		20%	70%	10%

Table 3: Categories

Question	Category
Do you pay attention to security certificates?	Attention
Do you use privacy granulation or attempt to control who can see particular information about you on the Internet? (e.g. friend lists in Facebook)	Privacy
Do you read EULAs (End User License Agreements) when installing software?	Attention
Have you ever received a harassing message through a social networking site?	Recipient
Do you read warnings, prompts, before clicking Yes/No?	Attention
Have you ever downloaded music/movies/media without paying for it?	Actions
Have you used text/code/images from the Internet without citing credit?	Actions
Have you attempted to find information on an individual for personal reasons, using the Internet?	Actions/Privacy
Have you used someone else's unsecured wireless connection?	Actions/Privacy
Have you looked through someone else's email/account/files/computer?	Actions/Privacy
Are you concerned about the amount of information about you available on the Internet?	Privacy
Have you ever installed software you didn't purchase (excluding Freeware, Open Source, etc.)?	Actions
Have you ever tried to damage someone's reputation using some form of technology (status updates, web page, mass email, posting pictures)?	Actions
Have you ever seen the above done to someone, but weren't involved?	Attention/Recipient
Do you read the Terms of Service when you sign up online for a service (like Google Sites, web hosting, email account, online banking)?	Attention
Do you apply the same moral, ethical and legal beliefs digitally that you believe in otherwise?	Belief
Did any teachers in high school discuss questions like those addressed in this survey?	Recipient
Have you ever seen someone else doing something "wrong" on a computer and said nothing to them or a teacher/supervisor/manager?	Actions/Belief
Do you use public computers for personal reasons?	Privacy/Actions
Do you set your email or other accounts to stay "signed in" for extended periods of time?	Privacy/Actions